Multi-Photon Entanglement Concentration and Quantum Cryptography

Gabriel A. Durkin, Christoph Simon, and Dik Bouwmeester
Centre for Quantum Computation, University of Oxford, Oxford OX1 3PU, United Kingdom
(Dated: January 29, 2002)

Multi-photon states from parametric down-conversion can be entangled both in polarization and photon number. Maximal high-dimensional entanglement can be concentrated from these states via photon counting. This makes them natural candidates for quantum key distribution, where the presence of more than one photon per detection interval has up to now been considered as undesirable. We propose a simple multi-photon protocol for the case of low losses and point out the robustness of the entanglement under photon loss.

Parametric down-conversion is a convenient way of creating entangled states of light [1]. So far it has been explored in two separate regimes. Experiments on the few-photon level have mostly relied on polarization entanglement [2], while experiments with macroscopic amounts of light have observed two-mode squeezing, that is entanglement in photon number [3].

It is however possible to build sources that combine both kinds of entanglement. The basic principle of such a source has recently been demonstrated [4]. Such a source can be seen as a pair of superimposed two-mode squeezers. We show that from this point of view photon counting can be used as a post-selective realization of entanglement concentration for continuous variable states, following the proposal of [5]. Maximal high-dimensional entanglement can be extracted in this way from the multi-photon states.

It is natural to consider the application of this entanglement for quantum key distribution. For the original quantum cryptography protocols [6, 7] the presence of more than one photon in a single pulse or detection interval is a problem for security. Therefore implementations of key distribution [8] are usually restricted to weak transmission signals, with a low probability of containing even a single photon, limiting the achievable bit rate per pulse. The pulse rate itself is mainly limited by the dead time of the photon detectors.

Here we take a more positive approach to multi-photon states in cryptography. We ask whether they can be used to improve the capacity of the secure channel. We propose a simple protocol which leads to a large increase in bit rates for the case of low losses. We also show that the entanglement is quite robust under photon loss, suggesting that more complex protocols may still be advantageous for higher losses.

We will first describe our proposed post-selective realization of entanglement concentration for continuous-variable states. Entanglement concentration is a procedure that allows two parties Alice and Bob to extract maximal entanglement from non-maximally entangled pure states using only local operations and classical communication [9]. Consider the (un-normalized) two-mode squeezed state

$$|\psi_1\rangle = \sum_{l=0}^{\infty} \lambda^l |l\rangle_{a_h} |l\rangle_{b_v} \tag{1}$$

where λ is usually referred to as the squeezing parameter. For later convenience, we have assumed that the photons in the spatial mode a (going to Alice) are horizontally and those in mode b (going to Bob) are vertically polarized. This state represents photon-number entanglement between modes a_h and b_v, that is, a quantum superposition of states for which the number of photons in mode a_h and b_v are the same. The state is however not maximally entangled since λ is always smaller than unity and therefore the individual terms in the superposition have different weights.

Based on ref. [5] we describe a way to concentrate photon-number entanglement. Suppose that in addition to (1) Alice and Bob are also given the state $|\psi_2\rangle = \sum_{m=0}^{\infty} (-\lambda)^m |m\rangle_{a_v} |m\rangle_{b_h}$, which differs from (1) by the sign of the squeezing parameter and by the polarization of the photons in modes a and b. The total state is then given by:

$$|\Psi\rangle = |\psi_1\rangle|\psi_2\rangle = \sum_{l=0}^{\infty} \sum_{m=0}^{\infty} \lambda^{l+m} (-1)^m |l\rangle_{a_h} |m\rangle_{a_v} |m\rangle_{b_h} |l\rangle_{b_v} . \tag{2}$$

Defining $n = l + m$, rearranging terms and using the short-hand notation $|u, v; w, x\rangle$ for $|u\rangle_{a_h}|v\rangle_{a_v}|w\rangle_{b_h}|x\rangle_{b_v}$ yields

$$|\Psi\rangle = \sum_{n=0}^{\infty} \lambda^n \left(\sum_{m=0}^{n} (-1)^m |(n-m), m; m, (n-m)\rangle \right) , \tag{3}$$

where we have collected the terms with the same number of photons n received by Alice and Bob.

Entanglement concentration is now achieved by performing a projection measurement onto a specific photon number. For a given n, this results in a superposition state of $n+1$ equally weighted terms. The concentrated entanglement is in the difference between the number of

horizontally and vertically polarized photons in modes a and b. The perfect quantum correlation is expressed as

$$(N_v - N_h)_a = (N_h - N_v)_b \,. \tag{4}$$

At first glance, the above scheme seems to require a quantum non-demolition (QND) measurement of the photon number on each side in order to project onto a fixed value of $n = (N_v + N_h)_a = (N_v + N_h)_b$ without losing the possibility of measuring $(N_v - N_h)_a$ and $(N_h - N_v)_b$ afterwards. Ways of realizing such a QND measurement were discussed in [5], but it is definitely not easy to implement.

On the other hand, *destructive* photon counting is feasible. It is therefore important to realize that for many applications it is not strictly necessary to perform the n projection before the $(N_v - N_h)_a$ and $(N_h - N_v)_b$ measurements. They can be performed simultaneously by simply measuring $(N_v)_a$, $(N_h)_a$, $(N_h)_b$ and $(N_h)_b$ independently. The basis of polarization analysis can be varied, allowing one to infer the projected value of n as well as extract information about the entanglement. This approach is similar to the post-selection strategy that enabled the demonstration of quantum teleportation [10] and related single-photon experiments.

Clearly, one should be careful in referring to a post-selection method as a concentration scheme since no concentrated output state is obtained. However, for the purpose of quantum cryptography the post-selection method will suffice, since it allows to establish perfect correlations between Alice's and Bob's measurement results.

For quantum key distribution, it is not sufficient to have perfect correlations in one specific basis. To prevent eavesdropping it is important that perfect correlations are also obtained in another *complementary* basis. We now show that, due to our specific choice of relative phases, the state (3) is rotational symmetric and therefore exhibits the same photon-number difference correlations in, for example, the linear polarization basis rotated by 45°. We also show how the state (3) can be generated in a natural way using type-II parametric down-conversion.

Parametric down-conversion is a process where a photon from a pump light source can be split into two photons of lower frequency within a non-linear optical crystal. One can experimentally achieve conditions where a good approximation for the relevant interaction Hamiltonian is

$$\hat{H} = \kappa(\hat{a}_h^\dagger \hat{b}_v^\dagger - \hat{a}_v^\dagger \hat{b}_h^\dagger) + h.c., \tag{5}$$

where the complex number κ is the product of the amplitude of the pump beam and the relevant non-linear coefficient of the crystal. This is the familiar Hamiltonian for the creation of polarization entangled photon pairs [2], which has been the basis for many experiments in quantum information. Using the normal ordering theorem of [11] one can show that this Hamiltonian leads to the production of entangled photon states of the following form:

$$\begin{aligned} |\psi\rangle &= \exp(-i\hat{H}t/\hbar)|0\rangle \\ &= \frac{1}{\cosh^2(\tau)} \sum_{n=0}^{\infty} \sqrt{n+1}\, \tanh^n(\tau)\, |\psi_-^n\rangle, \end{aligned} \tag{6}$$

where $\tau = \frac{\kappa t}{\hbar}$ is the effective interaction time and

$$\begin{aligned} |\psi_-^n\rangle &= \frac{1}{\sqrt{n+1}} \frac{1}{n!} (\hat{a}_h^\dagger \hat{b}_v^\dagger - \hat{a}_v^\dagger \hat{b}_h^\dagger)^n |0\rangle \\ &= \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)^m |(n\text{–}m), m;\, m, (n\text{–}m)\rangle \,. \end{aligned} \tag{7}$$

The total state (6) has exactly the form of state (3). The terms $|\psi_-^n\rangle$, which correspond to n photons on each side, are maximally entangled states shared between Alice and Bob in a Hilbert space of $(n+1) \times (n+1)$ dimensions. Similar states were studied in the context of Bell's inequalities in [12]. They are all invariant under joint identical polarization transformations by Alice and Bob, since they are created by the application to the vacuum of powers of the operator $(\hat{a}_h^\dagger \hat{b}_v^\dagger - \hat{a}_v^\dagger \hat{b}_h^\dagger)$, whose form is conserved under such transformations. These properties make them generalized singlet states, which motivates our notation $|\psi_-^n\rangle$. Whenever Alice has $(n-m)$ photons polarized along a certain direction and m photons polarized along the orthogonal one, Bob has m and $(n-m)$ photons of the respective polarizations. When employed for quantum key distribution, every pair of values $(m, n-m)$ constitutes a letter in the cryptographical alphabet.

A simple key distribution protocol using the multi-photon states proceeds in the following way. From a common source, entangled multi-photon pulses are sent to Alice and Bob via modes a and b. Alice and Bob each independently and randomly choose the basis, H/V or $45°/-45°$, in which to perform their photon number measurements. These measurements act as a multi-photon entanglement concentration resulting in detected correlations associated to the states $|\psi_-^n\rangle$, where n is the number of detected photons on each side. They communicate their basis choice via classical means and extract the key from the photon number difference recorded in those cases where they had chosen the same basis. Finally they compare a randomly chosen part of the key to detect whether an eavesdropper has been present. Eavesdropping will affect the maximal entanglement and thus introduce errors.

It is clear that in the absence of losses and errors the achievable bit rate increases significantly with the number of photons because the number of distinguishable results increases. There are $n+1$ different possible measurement results for the state $|\psi_-^n\rangle$. For protocols based on the multi-photon states $|\psi_-^n\rangle$, losses introduce errors because they affect the entanglement. In quantum key

distribution, in principle one has to assume that all errors could be due to eavesdropping. The achievable secure bit rate or *secrecy capacity* [13] C_s in the presence of an eavesdropper Eve is bounded from below by the inequality

$$C_s \geq I_{AB} - \min(I_{AE}, I_{BE}), \tag{8}$$

where I_{XY} is the mutual information between parties X and Y. The mutual informations and therefore also the bound on the secrecy capacity depend on the type of attack employed by the eavesdropper. Determining the achievable secure bit rates under lossy conditions therefore requires an analysis of possible eavesdropping strategies. This is not an easy task in the present situation since the system under consideration is complex, and the effectiveness of a particular eavesdropping strategy depends on the precise protocol chosen.

In this paper, as a first step, we consider a protocol where Alice and Bob make use of the 4-photon detection results (each detects 2 photons) in addition to the 2-photon results (each detects 1 photon). We have compared this case to the standard protocol where only the 2-photon results are used [8].

We suppose that Eve's technological capabilities are so powerful that she can replace the lossy transmission lines between Alice and Bob by ideal lossless ones. Furthermore, Eve is in control of the source. Sometimes she simply distributes the states $|\psi_-^1\rangle$ and $|\psi_-^2\rangle$ to Alice and Bob, but sometimes she first performs a measurement on them in one of the bases utilized by Alice and Bob. The important constraint on Eve's operations is that in order to avoid being detected she has to pretend to Alice and Bob that the errors observed by them are actually caused by losses. Eve mimics a certain combination of losses and source strength, i.e. effective interaction time τ. Firstly this means that she also has to send signals containing photon numbers other than 2 and 4 with appropriate probabilities. Secondly she has to choose the percentage of cases in which she actually performs a measurement on the states $|\psi_-^1\rangle$ and $|\psi_-^2\rangle$, such that the level of errors introduced by her measurement corresponds to the level of errors expected by Alice and Bob.

Under these conditions one can determine the bound on the secrecy capacity (8) as a function of the losses and of τ. The results are shown in figure 1. One sees that for a comparatively low level of losses the secrecy capacity, or more precisely the lower bound on it, is approximately doubled by using the 4-photon states in addition. This effect would be increased substantially by including higher photon numbers.

It should be noted in this context that highly efficient photon-counting detectors [14] and optical fibres with very low losses [15] are both under development. At the present stage, losses and limited detection efficiencies are serious practical restrictions. One can see from fig. 1(b) that for the present protocol the advantage of using the higher photon number states disappears for overall losses that exceed 20 percent. For larger losses the error probability becomes so high that no secret key can be distilled.

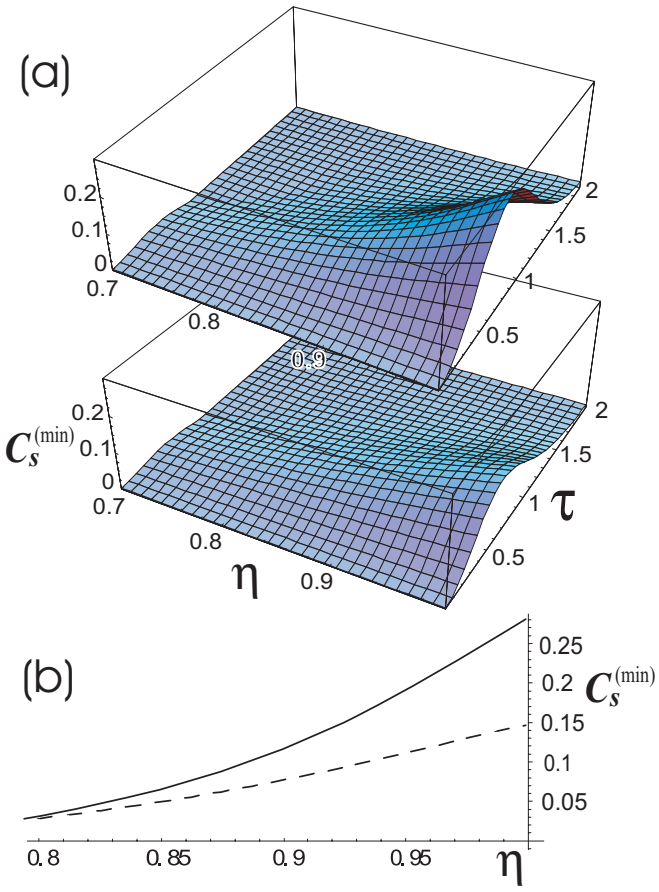

FIG. 1: Both graphs show the lower bound Eq. (8) on the achievable secure bit rate C_s. In (a) it is plotted as a function of η and τ, where η is the overall transmission, encompassing limited detection efficiency and propagation losses, and τ is the effective interaction time of the source, cf. Eq. (6). The upper plot of (a) refers to the protocol using both 2-photon and 4-photon results, while the lower plot is for the standard protocol using 2-photon results only. One sees that using 4-photon detections in addition leads to a significant increase in secure bit rates in the region of low losses. This is shown in more detail in (b) where we have plotted the lower bound on C_s for both protocols, at their optimal τ values; $\tau = 0.78$ and $\tau = 0.70$ for the new and old protocols respectively. The bound on C_s decreases for higher τ values, as can be seen clearly in (a), because the probabilities for 2-photon and 4-photon results are reduced as higher photon numbers become more and more likely. Including them would further increase the achievable bit rates.

However, there is some indication that the multi-photon states may still be viable candidates for quantum key distribution for higher losses, if more elaborate protocols are considered. From the point of view of quantum communication in general, a natural question to ask is how the entanglement in the considered multi-photon

states is affected by photon loss. It turns out to be surprisingly robust, as illustrated by the following example. Consider the four-photon state

$$|\psi_-^2\rangle = \frac{1}{\sqrt{3}}(|2,0;0,2\rangle - |1,1;1,1\rangle + |0,2;2,0\rangle) \qquad (9)$$

If the environment does not preferentially absorb photons of a specific polarization, then the loss of a photon of unknown polarization in spatial mode a from a state with density matrix ρ is described by the following simple transformation:

$$\rho \to L_a(\rho) = \frac{1}{\langle N_a\rangle}(a_h \rho a_h^\dagger + a_v \rho a_v^\dagger), \qquad (10)$$

where $\langle N_a\rangle = \mathrm{Tr}\rho(a_v^\dagger a_v + a_h^\dagger a_h)$ is the normalization constant. Note that because of its scalar-product-like form the loss map L_a does not depend on the polarization basis chosen. It commutes with arbitrary polarization transformations and thus does not change the symmetry properties of ρ under such transformations. The same holds for the analogously defined map L_b corresponding to losing a photon of unknown polarization in spatial mode b.

Let us now consider the two-photon state that is obtained from the four-photon state $|\psi_-^2\rangle$ by losing one photon on each side, i.e. the state $L_a \otimes L_b(|\psi_-^2\rangle\langle\psi_-^2|)$. From the invariance of $|\psi_-^2\rangle$ under bilateral polarization transformations and the above-mentioned symmetric character of the losses it follows that this state must be of the general form

$$\beta|\psi_-\rangle\langle\psi_-| + \frac{1-\beta}{4}\mathbb{1}, \qquad (11)$$

i.e. it is a two-qubit Werner state, where

$$|\psi_-\rangle = |\psi_-^1\rangle = \frac{1}{\sqrt{2}}(|1,0;0,1\rangle - |0,1;1,0\rangle). \qquad (12)$$

The qubits correspond to the two polarization states of the remaining single photon in either spatial mode.

Straightforward application of L_a and L_b to $|\psi_-^2\rangle$ gives $\beta = 2/3$. Using the well-known partial transposition criterion for separability [16], one can easily show that states of the form (11) are entangled for $\beta > 1/3$. This implies that the state $L_a \otimes L_b(|\psi_-^2\rangle\langle\psi_-^2|)$ still contains a substantial amount of entanglement, which could e.g. be distilled to singlet form [17] and then used for cryptography or other quantum communication tasks. A potential method for the purification of polarization entangled photons has recently been suggested [18].

The inseparability of the two-photon state implies of course that the states obtained from $|\psi_-^2\rangle$ by losing only one photon are also entangled and distillable. We will perform a more general analysis of how the entanglement in the states (6) is affected by photon loss in a future publication.

There are other natural applications for multi-photon entanglement besides quantum key distribution, such as all-optical quantum error correction [19], or even all-optical quantum computation [20]. The use of the down-conversion multi-photon states for these purposes is a topic for future research.

We thank G. Giedke and L. Vaidman for stimulating discussions. This work was supported by the EPSRC GR/M88976 and the European Union QuComm (IST-1999-10033) projects.

[1] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information* (Springer, Berlin, 2000).
[2] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[3] Z.Y. Ou, S.F. Pereira, H.J. Kimble, and K.C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).
[4] A. Lamas-Linares, J.C. Howell, and D. Bouwmeester, Nature **412**, 887 (2001).
[5] L.M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 4002 (2000).
[6] C.H. Bennett and G. Brassard, Proc. IEEE Int. Cnf. on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179 (1984)
[7] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
[8] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett **84**, 4729 (2000); D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, P.G. Kwiat, Phys. Rev. Lett **84**, 4733 (2000); W. Tittel, J. Brendel, H. Zbinden, N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[9] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[10] D. Bouwmeester *et al.*, Nature **390**, 575 (1997).
[11] D.R. Traux, Phys. Rev. D **31**, 1988 (1985).
[12] P.D. Drummond, Phys. Rev. Lett. **50**, 407 (1983).
[13] For an introduction to the concept of secrecy capacity see A.K. Ekert, B. Huttner, G.M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994) and references therein.
[14] J. Kim, S. Takeuchi, Y. Yamamoto, and H.H. Hogue, Appl. Phys. Lett. **74**, 902 (1999); S. Takeuchi, J. Kim, Y. Yamamoto, and H.H. Hogue, Appl. Phys. Lett. **74**, 1063 (1999).
[15] R.F. Cregan *et al.*, Science **285**, 1537 (1999).
[16] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[17] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[18] J.-W. Pan, C. Simon, Č. Brukner, and A. Zeilinger, Nature **410**, 1067 (2001).
[19] D. Bouwmeester, Phys. Rev. A **63**, 0301 (2001).
[20] E. Knill, R. Laflamme, and G.J. Milburn, Nature **409**, 46 (2001).